Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
	)	
	)	
Implementation of Section 304 of the	)	
Telecommunications Act of 1996	)	**CS Docket No. 97-80**
	)	
Commercial Availability of	)	
Navigation Devices	)	
	)	
	)	
	)	
	)	
	)	
	)	
	)	
	)	

COMMENTS OF THE
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

C. Bradley Hunt
Executive Vice President and
Chief Technology Officer
Motion Picture Association of America, Inc.
15503 Ventura Boulevard
Encino, California 91436
(818) 995-6600

February 6, 2006

	)	
	)	
In the Matter of	)	
	)	
Implementation of Section 304 of the	)	
Telecommunications Act of 1996	)	**CS Docket No. 97-80**
	)	
Commercial Availability of	)	
Navigation Devices	)	
	)	
	)	

COMMENTS OF THE
MOTION PICTURE ASSOCIATION OF AMERICA, INC.

INTRODUCTION

The Motion Picture Association of America, Inc. ("MPAA") and its member companies submit the following comments in response to the comments of (1) ATI Technologies, Inc. ("ATI") , Dell, Inc. ("Dell"), Hewlett-Packard Company ("H-P"), and Intel Corporation ("Intel") (collectively "the Computer Companies") submitted to the FCC on January 20, 2006 and the comments of (2) Dell, H-P, Intel, & Sony Electronics, Inc., submitted on January 20, 2006.

The MPAA supports the development of the DCAS technology and its implementation in a wide range of cable navigation platforms, including general-purpose computers, which can support greater consumer utility of cable-delivered content and a more competitive marketplace for cable navigation devices. It is important that the security elements of DCAS be implemented in a consistent manner across all cable navigation platforms to ensure that high-value, copyrighted content is never exposed to unauthorized copying and/or redistribution.

1.   The PCI Express Interconnect Bus Should Be Considered a "User Accessible Bus" and The Interface Between Discrete Decryption Engines and Discrete Video Decoders Must Be Protected.

The Computer Companies claim that it would be difficult for one to access cable content on the PCI Express interconnect bus. However, they do not assert that it is an unachievable task given sufficient development time and resources. Specifically, the Computer Companies have not claimed, and cannot claim, that it would be impossible to manufacture a tool to gain access to Controlled Content that travels in the clear over a PCI Express interconnect bus. Indeed, one could imagine a PCI Express Card, developed and sold legitimately as a PCI Express bus analyzer. This card could be used in combination with a downloaded software application to easily access in-the-clear Controlled Content moving across the PCI Express bus. The possibility that such a tool could be developed to access Controlled Content supports CableLabs' position that the PCI Express is a "user accessible bus."

There is an additional harm to content providers if Controlled Content is not protected while moving across the PCI Express bus. If, as suggested by the Computer Companies, there were no such protection applied to Controlled Content moving over this bus, then one could argue that there is no "technological measure" being applied as defined under the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2005) (the "DMCA") and that the DMCA protections would be unavailable. *See* 17 U.S.C. §1201. Therefore, the MPAA believes that the DCAS license agreement should not be amended to eliminate the categorization of the PCI Express interconnect bus as a user-accessible bus.

Likewise, Controlled Content traveling across a PCI Express bus between a discrete

DCAS decryption engine and a discrete video decoder residing in the software player application

must be encrypted, or otherwise protected,[1] from being accessed in the clear. Without such a

"technological measure," content providers may be deprived of the protections afforded under

the DMCA. While the MPAA supports enabling general-purpose computers as secure, cable

navigation devices through their incorporation of the DCAS technology, the MPAA disagrees

with the Computer Companies' position to eliminate the current DCAS license requirement that

the interface between discrete decryption engines and discrete video decoders be encrypted.

2.   An Effective Downloadable Conditional Access System Must Have a Hardware
Root of Trust.

DCAS can only operate effectively in the form of authenticated software loaded and

executed within a DCAS Secure Microprocessor Chip since the system relies upon a hardware

"root of trust" within the specialized microprocessor Chip. DCAS cannot provide the same level

of security if it were to be implemented in the form of a software application that was

downloaded and executed on a general purpose computer, as suggested in the comments filed by

Dell, H-P, Intel and Sony Electronics, Inc. In fact, if DCAS were implemented as a

downloadable software application with a software "root of trust," it would greatly expose the

security of the system to software attacks, which could be developed and easily distributed over

the Internet.

---

[1] Although encryption is well-recognized as a secure means of protecting a stream of Controlled Content,
the MPAA and its member companies would be amenable to discussing other effective technological measures to
protect Controlled Content.

The MPAA restates its support of the goal of Dell, H-P, Intel and Sony Electronics, Inc. in enabling the general purpose computer as a cable navigation platform to enhance the competitive marketplace for navigation devices. However, the MPAA does not see the need to eliminate the security afforded by the DCAS Secure Microprocessor and its hardware "root of trust" as necessary to achieve this goal.

3.   DCAS Should Support Secure Home Networking of Cable-Delivered Content.

The MPAA has supported technological innovations that enable secure home networking because they provide benefits to both cable subscribers and content providers. In that vein, the MPAA supports the position reflected in the comments filed by Dell, H-P, Intel and Sony Electronics, Inc. that DCAS should recognize and support secure home networking.

To this end, the MPAA has worked with CableLabs to gain its support for additional protection technologies to enable secure home networking of cable-delivered content. For example, on July 11, 2005, the MPAA filed a joint letter of support with the Digital Transmission Licensing Administrator, LLC ("DTLA") to CableLabs to support the approval of DTCP over IP as an authorized digital output protection technology. This was done in conjunction with gaining CableLabs' support for implementing a Redistribution Control Trigger ("RCT") bit that would signal when redistribution control is asserted over Controlled Content where no numeric copy control is being asserted. Since the RCT bit was implemented in the DCAS License, the MPAA and its member companies support the approval of DTCP over IP as an authorized output technology under the DCAS License.
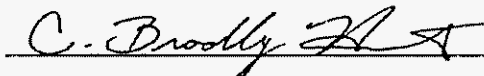
CONCLUSION

The MPAA supports the development of the DCAS technology and its implementation in a wide range of cable navigation platforms, including general-purpose computers. However, the MPAA does not see the logic or the need to lower the security requirements for computer-based platforms in order for them to successfully compete in the navigation device marketplace. The MPAA also supports secure home networking of cable-delivered content and strongly urges CableLabs to amend the DCAS License to support the approval of DTCP over IP as an authorized digital output protection technology.

Respectfully submitted,

THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.

By:

C. Bradley Hunt
Executive Vice President and
Chief Technology Officer
Motion Picture Association of America, Inc.
15503 Ventura Boulevard
Encino, California 91436
(818) 995-6600